## REMARKS

The above amendment and these remarks are responsive to the Office Communication of Examiner Victor D. Lesniewski, mailed 10 Jun 2005, and designated as non-Final.

Claims 1-5, 8-14, 18-25, 29-30, 34-41, 43, and 45 -53 are in the case, none as yet allowed.

### *35 U.S.C. 101*

5. Claims 44 and 49-53 have been rejected under 35 U.S.C. 101 as directed to non-statutory subject matter.

Applicant has canceled claim 44, which, when corrected, would be redundant with respect to claim 49.

Applicant has amended claims 49-53 to recite a computer readable medium, and requests that the rejection of these claims under 35 U.S.C. 101 now be withdrawn.

### *35 U.S.C. 102*

8. Claims 1-4, 6, 8, 10-14, 34, 36, 37, 43-45, 49, and 50 have been rejected under 35 U.S.C. 102(e) over Lucovsky (U.S. Patent 6,868,450).

In the present invention, IP packet filtering occurs in an operating system kernel implementation of, for example, the TCP/IP protocol suite. Access rules are expressed as filters referencing system kernel data; for outbound processing, source application indicia is determined; for

inbound packet processing, a look-ahead function is executed to determine target application indicia; and responsive to the source or target application indicia, filter processing is executed.

There are some similarities between the current application and Lucovsky. They are both in the same general area of IT technology, having to do with network communications and the filtering of networking traffic. Both assume packet-switched networking protocols (Lucovsky explicitly mentions TCP/IP). And, among the actions that follow filtering, there are some expected similarities. For example in the ability to reject a protocol packet in some fashion; that is, not allow it to continue in a normal (non-filtered) manner.

But the manner of operation, including key particulars, appear different.

Applicant represents that certain limitations in claim 1, as well as in all independent claims presented in the current application, which are not in Lucovsky include 'filters referencing system kernel data', and 'a look-ahead function to determine target application indicia'.

It is instructive to an understanding of the differences between Lucovsky and the present application to consider elements of Lucovsky not included or required by the present invention. These include, referring to Col. 2, lines 13-35; Col. 7, lines 51-65; Col. 8, lines 23-32; Col 8, lines 11-16 and 33-40, "an API in communication with the software process", "a network attribute", "a system call

trap handler", the trap handler "configured to learn the process attribute and the network attribute", "a session filter driver", "a database associated with the session filter driver", another database associated with the system call trap handler (Fig. 2, element 118), and Col. 7, lines 51-65, 'a network filter driver'.

Since all these parts of Lucovsky are not in the current application, the current invention is not required to, that is, avoids the necessity to, execute such actions as in Col. 7, lines 51-65 'intercepts the TCP/IP packets from the TCP/IP driver', 'obtain the local process address ... from the intercepted packet', 'queries the database', 'obtain the attribute associated with the local process'. And for Col. 8 (all lines), these elements are not required by the present invention: 'the system call trap handler is queried', 'this decision is made by comparing the process attribute ... that was retrieved from the database with the network attribute of the NIC', 'obtains the local process endpoint from the packet' [this appears to refer to the destination port in the transport protocol header (TCP or UDP) of the packet], 'the network filter driver using the local process endpoint...', 'obtain the attribute ... from the database'. And finally, 'the network filter driver queries the system call trap handler', 'this decision is made by comparing the process attribute ... retrieved from the database ... with the NIC attribute'.

Note that last line; "comparing the process attribute ... with the NIC attribute". This is the full extent of Lucovsky filtering capabilities (see for example Lucovsky claim 1, col 11 8-42). Two attributes are tested for

equality.

In contrast, claim 1 of the present invention, which states "executing filter processing", is referring to full-function generalized filtering as described in applicants specification, as follows:

> "Referring to Figure 3, as an extension to normal IP protocol functions, filtering examines each packet 140 by comparing it against a set of filter rules 166. Each filter rule 166 contains a set of 'selectors' 160, each of which specifies a certain field in the packet 140 and some set of values 164, and an operator 162 for performing a match operation. A filter rule 'matches' a packet 140 (and the packet 'matches' the filter rule) when each of that filter's selectors, when checked against the packet, returns 'true'. (A filter rule may have 0 or more selectors, each with associated operator and value set.)" [Specification, page 8, line 12 to page 9, line 2].

> "Referring to Figure 7, which is Figure 1 of U.S. Patent 6,182,228, the key elements and logical relationships and data flow among them, are illustrated for translating FILTER statements 100 to a 6-tuple representation 124, and interpreting them as IP datagrams flow through the OS kernel 120." [Specification, page 18, lines 15-21].

The term "operator" is defined in the above identified related U.S. Patent 6,182,228 B1, as follows:

"Referring to Figure 3, the logical structure of each 6-tuple includes operator 200, nextrule 202, offset 204, value 1 206, value 2 208 and value 3 210.

(operator, nextrule, offset, value1, value2, value3)

Operator 200 represents a logical operation to be performed (e.g. tests such as '=', '<=', etc.) As generated by compiler 102 during invocation 104, this is a function index, that is resolved to a function pointer during invocation 114 for loading to memory..." [U.S. Patent 6,182,228 B1, Col. 3, line 59 to Col. 4, line 2].

Therefore, applicant's reference to "filter processing" has these implications; logical expressions of arbitrary length are constructed and evaluated, using a set of logical operators, and allowing many alternatives for a filter selector field and value set (which in U.S. Patent 6,182,228 B1 includes value1, value2, value3).

In contrast, Lucovsky has one operator (equals), one logical expression (A equals B), and two pre-defined selector values (process attribute and NIC attribute).

In broader terms, Lucovsky appears to solving a much narrower problem than the present invention, as shown in Col. 2, lines 1-6 and Col. 11, lines 34-40. Namely "to drop the communications packets if the system call trap handler determines that the software process is not authorized access to the network interface card." (Col. 11,

lines 36-39). And this problem is solved with data (his two databases (Fig. 2, elements 115, 118) and parts (system call trap handler, session filter driver, and others) that are absent from and not required by the present invention.

In contrast, the present invention does filtering in the broad sense (see, for example, applicant's Fig. 3 and related description), without any databases referenced from kernel space (Fig. 7 and related description), and without most of the elements that Lucovsky requires (see above).

The Examiner states that Lucovsky discloses "for inbound packet processing, executing a look-ahead function to determine target application indicia (column 8, lines 23-32)". [Office Action, pages 3-4, and 12]. Lucovsky teaches:

> "When receiving packets via network 11, the network filter driver 140 intercepts the TCP/IP packets from the network driver 113 and obtains the local process' endpoint (destination) from the packet. The network filter driver 140, using the local process' endpoint address, accesses a database 115 via connection 162 to obtain the attribute associated with the receiving process. For example, if the process 101 is the receiving process, then the process attribute 119 (NetAttr) would be obtained by the network filter driver 140 from the database 115." [Lucovsky, Col. 8, lines 23-32.]

Lucovsky refers to an endpoint address as the set of {protocol, port number, IP address}, which is managed by the

TCP/IP driver "in what will be referred to as a network object (for example in a socket structure...)" [Col. 5, lines 24-32.] However, Lucovsky uses that endpoint address to access database 115 to obtain the process attribute, and does not teach obtaining from the socket layer any indicia identifying the application layer application to which an inbound packet marked non-deliverable would have been delivered.

Thus, the Lucovsky process is not the same process as that to which applicant refers as "look-ahead" processing. However, it is apparent that the distinction needs to be clarified in applicant's claims.

Applicants look-ahead process is described as follows:

"To determine the target application 31 for inbound processing, a look-ahead function is executed. According to that look-ahead function, the filter function asks the sockets layer to identify the application 31 to which it would give the packet, but that packet is at this point in the process marked as non-deliverable." [Specification, page 15, lines 14-19.]

"Referring further to Figure 5, in connection with Figure 6, which describes how the look-ahead function described hereafter fits within the TCP/IP protocol stack 80, architecture inbound packet 50 processing differs from outbound packet 60 processing primarily in that the task of the caller of filtering is not identified to a user-space 92 process 81, 82, etc.,

that should receive packet 50. This inbound processing only applies to packets destined for the system doing the filtering, and requires a new IP-level function 100."

"In step 52, from the filtering function 90 at the IP-layer 99, invoke a new transport-layer 96 TCP 83, UDP 84, or RAW 85 'look-ahead' (LA) function 87-89, respectively, by passing the transport-layer 96 header and, if necessary, also the IP protocol 99 header. Which transport-layer 96 look-ahead function 83-85 to call is determined by the IP layer 99 header ip_p field. The selected look-ahead function 83-85 determines which user-level process or job 81-82,..., will receive the packet later, when the packet is sent to the transport layer 96. The task id of the corresponding process 81-82 is returned." [Specification, page 17, line 10 to page 18, line 9.]

Thus, look ahead processing is executed within a protocol stack including an IP layer, a transport layer, a sockets layer, and an application layer in which, for an inbound packet, the IP layer provides to the transport layer a packet marked as non-deliverable, and receives back from the transport layer indicia provided to the transport layer by the sockets layer identifying the application layer application to which the packet would have been delivered.

Applicants have amended all independent claims (dealing with inbound processing) to clarify the above concept of 'look-ahead' processing.

New features of the present invention, which are not taught or anticipated by Lucovsky, are the full-function filtering, referencing data in the kernel (not just the packet) and not in databases, and which, with the look-ahead function, allows filtering of non-IP packet data, as well as IP packet data, for all inbound and outbound traffic.

So, the positioning of -0019 and Lucovsky is that Lucovsky solves a very small subset of problem space addressed by -0019, and -0019 does most things differently.

Claim 1 and all other independent claims have been amended to recite the above concept of filter and look-ahead processing, and thus distinguish Lucovsky.

Applicants, therefore, urge that the rejections under 35 U.S.C. 102 be withdrawn, and claims 1-4, 8, 10-14, 34, 36, 37, 43, 45, 49, and 50 be allowed.

***35 U.S.C. 103***

Claims 5, 7, 9, 22, 24-33, 35, 39, 41, 42, 47, 48, 52, and 53 have been rejected under 35 U.S.C. 103(a) over Lucovsky.

Claims 7, 26-28, 31-33, and 42 have been canceled.

Claims 5, 9, 22, 24, 25, 29, 30, 35, 39, 41, 47, 48, 52, and 53 have been amended (directly, or by reference to parent or intermediate claims) to set forth the more limited distinctions above described with respect to filtering and look-ahead processing and which, applicant represents, now

meet the requirements of allowability under the statute with respect to Lucovsky, as described above.

Claim 15 has been rejected under 35 U.S.C. 103(a) over Lucovsky in view of Wiegel (U.S. Patent 6,131,163).

Applicants have canceled claim 15.

Claims 16-21, 23, 38, 40, 46, and 51 have been rejected under 35 U.S.C. 103(a) over Lucovsky in view of Fiveash et al. (U.S. Patent 6,076,168, hereinafter Fiveash).

Claims 15, 16, and 17 have been canceled.

Claims 18-21, 23, 38, 40, 46, and 51 have been amended (directly, or by reference to parent or intermediate claims) to set forth the distinctions above described with respect to filtering and look-ahead processing, and thus distinguish Lucovsky. Further, while Fiveash is related, generally, to filtering, Fiveash does not provide look-ahead processing, as now set forth in the claims. Further, filtering is done by Fiveash only with respect to IP packet data, and not non-IP packet data as required by the claims, and thus, in combination with Lucovsky, does not teach the claims as currently presented with limitations relating to filtering of non-IP data and look-ahead processing.

Applicants, therefore, urge that the rejections under 35 U.S.C. 103 be withdrawn, and that claims 18-21, 23, 38, 40, 46, and 51 be allowed.

## SUMMARY AND CONCLUSION

Applicants urge that the above amendments be entered and the case passed to issue with claims 1-5, 8-14, 18-25, 29-30, 34-41, 43, and 45 -53.

The Application is believed to be in condition for allowance and such action by the Examiner is urged. Should differences remain, however, which do not place one/more of the remaining claims in condition for allowance, the Examiner is requested to phone the undersigned at the number provided below for the purpose of providing constructive assistance and suggestions in accordance with M.P.E.P. Sections 707.02(j) and 707.03 in order that allowable claims can be presented, thereby placing the Application in condition for allowance without further proceedings being necessary.

Sincerely,

Edward B. Boden

By

Shelley M Beckstrand
Reg. No. 24,886

Date: 9 Sep 2005

Shelley M Beckstrand, P.C.
Patent Attorney
61 Glenmont Road
Woodlawn, VA 24381-1341

Phone: (276) 238-1972
Fax: (276) 238-1545